REMARKS/ARGUMENTS

Claims 1-10 and 12-20 were pending. New claim 21 is entered, accordingly, claims 1-10 and 12-21 are now pending. Amendments were made to claims 1, 3, 8, 12, 15 and 20 for stylistic purposes, and do not affect the scope of the claims. Claim 17 was amended to clarify the claim language.

Claims 1-10 and 12-20 were variously rejected under 35 USC 103(a) in light of Yatsukawa an view of Baskey, and in view of Chang or Arthan.

I. THE PRESENT INVENTION

Embodiments of the present invention relate to secure computer network access.

As described in the Background of the Invention, prior methods to the invention for secure remote access have included use of electronic "key cards" or "tokens" to authenticate the client. P. 1, lines 24-28. As also described, drawbacks to such solutions include that these tokens only authenticate the bearer, and not the user. P. 2, lines 1-2. Another drawback is that that these tokens typically need to be manually pre-registered by a network administrator before they are activated. P. 1, lines 31-32. Yet another drawback is that these devices typically need to be synchronized with the server, otherwise the client will not authenticate. P. 2, lines 3-5.

Embodiments of the present invention address the problems without the drawbacks described above. In these embodiments, a user does not need to have a hardware or software "token" to gain network access and no registration or synchronization need be performed. Instead, the user only needs to have an authentic public/private key pair. In the embodiment illustrated in Figs. 4A-D, the user enters a correct password into a key wallet to retrieve their private key and digital certificate (steps 400-470). As an innovation, when the user enters an incorrect password, an invalid private key and a digital certificate are provided by the key wallet (step 480). As was explained, Step 480 is an example of an Arcot Systems brand "cryptographic camouflage" key protection technique. P. 7, lines 28-34. For further information about this technique, see U.S. Pat. No. 6,170,058.

In the various embodiments, the client then requests a one-time password from an external server, step 490. In response, the external server provides the one-time password, which is inactive, steps 500-530. Notice that before steps 500-530, the client does not have the one-time password.

Next, the client uses the received one-time password and digitally signs it with the private key to form a digital signature, step 540. The digital signature and the users digital certificate are then sent back to the external server, step 560. Subsequently, if the digital signature and digital certificate authenticate the user, the one-time password is activated, and the client may use the one-time password to access the protected computer network. Steps 570-690.

Certain features of the above embodiments are found in the claims. For example, Claim 1 recites code that directs the processor to receive the challenge from the authentication server via a first secure communications channel, wherein the challenge comprises an identity code, and code that directs the processor to form a digital signature in response to the identity code from the authentication server and the private key.

Additionally, dependent claim 5 recites wherein code that directs the processor to determine the private key and the digital certificate in response to the user authentication data further comprises code that directs the processor to determine a private key not associated with the user when the user authentication data is incorrect.

Claim 8 recites a processor coupled to the tangible memory, the processor configured to receive a challenge from an authentication server via a first secure communications channel, the challenge comprising an identity code, configured to receive user authentication data from the user, configured to determine a retrieved private key and a retrieved digital certificate from the key wallet in response to the user authentication data from the user; configured to form a digital signature in response to the identity code received from the authentication server and the retrieved private key, configured to communicate the digital signature to the authentication server, configured to communicate the digital certificate to the authentication server, and configured to communicate network user authentication data and the identity code to the authentication server via a security server.

Additionally, claim 10 recites wherein the retrieved private key and the private key associated with the user are different.

Further, claim 15 recites means for receiving a challenge from a verification server via a first secure communications channel, the challenge comprising at least a network password that is inactive, and means for forming a digital signature in response to the network password received from the verification server and to the private key.

Additionally, dependent claim 17, as amended, recites wherein the means for determining a returned private key comprises means for determining the returned private key in response to the PIN from the user, and a pre-determined PIN, wherein when the PIN from the user and the pre-determined PIN are different, the returned private key is different from the private key associated with the user, wherein when the PIN from the user and the pre-determined PIN are the same, the returned private key is the private key associated with the user.

II. THE CITED REFERENCES

A. Yatsukawa

Yatsukawa relates to an authentication system using information valid for one-time, by using a list of seed values Ds stored on both the client and the server.

As illustrated in Fig. 13, the Client system 204 includes "Original Data" Dn-1 as a function of Ds0. Additionally, the Server system 105 has therein "Inspection Data" Dn-1 as a function of Ds0. As described in the Yatsukawa, data D is "authentication-data inspection data," col. 15, line 51, and Ds0 is the initial "seed data" for authentication purposes. Col. 16, lines13-14.

In operation, initially, the client logs into a server, col. 16, lines 46-52. Next, the server sends an authentication-data request, col. 16, lines 54-55. Then, the client generates authentication data D by enciphering the seed data Ds0 by the client private key K, and then D is sent back to the server, col. 16, lines 57-60. The server then deciphers the authentication data D using the client public key K to recover the client seed data. col. 17, lines 1-14. Next, the server compares the recovered client seed data to Ds0 already stored in the server. Col. 17, lines 14-17.

In Yatsukawa for the first session Ds0 is used as the seed. For the next session, Ds1 is used for the seed, etc.

Accordingly, as illustrated above, Yatsukawa discloses a form of a "token" based system where the seed data must be synchronized with a server. A drawback to such a system includes that the client and server must pre-arrange a seed data list. Another drawback is that the client and server must be synchronized such that the client seed value used (e.g. Ds5) is the same as the server seed value used (e.g. Ds5).

B. Baskey

Baskey relates to a system using a Secure Socket Layer proxy server.

Baskey discloses nothing about authentication protocol.

C. Arthan

Arthan relates to public/private key management. More specifically, Arthan mentions that when a user's private key is compromised, a new public/private key pair should be generated for the user. The Examiner cites language in Arthan "If a key becomes compromised, then good cryptographic practice dictates that operational use of that key be suspended." Action, p. 10, lines 16-17.

Notably, Arthan does not disclose anything about a key wallet or what happens when a user enters an incorrect password into a key wallet to attempt to access a public/private key pair.

D. Chang

Chang relates to a token caching security system. In the Background of Chang it describes the use of a hardware token for generating a one time password. More specifically, Chang describes use of a "Smart card or Token card .. such as SecurID card commercially available from Security Dynamics, Inc.," that generates a series of one time passwords. Col. 2, lines 11-24. In use, the user enters data into the token card, and the hardware token generates a one-time password. Col. 2, lines 25-28. The user then submits the token generated one-time password to a password server 128 that is synchronized with the hardware token for verification. Col. 2, line 28-33.

Chang notes that is burdensome for a user to repeatedly use the hardware token to generate one time passwords, each time the user wants to log in. Col. 2, lines 52-60. Accordingly, Chang's purported innovation is to cache the user name and one-time password, so the user can log in at a later time without use of the hardware token. Col. 42-49.

Accordingly, Chang discloses a "token" based system where a hardware token must be synchronized with a server, and where the hardware token is used to generate a one-time password to allow a user access to a network.

III. THE CITED REFERENCES DISTINGUISHED

A. Claim 1

The elements of Claim 1 are not disclosed, suggested, or taught by Yatsukawa in view of Baskey. More specifically the cited references fail to disclose code that directs the processor to receive the challenge from the authentication server via a first secure communications channel, wherein the challenge comprises an identity code.

As discussed above, Yatsukawa is a form of "token-based" authentication where the client determines the authentication-data inspection data. Importantly, in Yatsukawa, the challenge from the server to the client does not include any seed data Ds0, as is recited above. In Yatsukawa, the client must already have a list of the seed data in memory. Further, the seed data for the client and the seed data for the server must be synchronized.

Further, the cited references fail to disclose code that directs the processor to form a digital signature in response to the identity code from the authentication server and the private key.

Again, at best, Yatsukawa forms a digital signature based upon the a priori known authentication-data inspection data and seed data Ds. Yatsukawa does not form a digital signature based upon data received in the challenge, as recited above.

These limitations are also not taught by Baskey, as discussed above.

Accordingly, these references fail to disclose all the elements of claim 1.

B. Claim 5

The elements of Claim 5 are not disclosed, suggested, or taught by Yatsukawa in view of Baskey and Arthan for the reasons discussed above for claim 1. Additionally, the cited references fail to disclose code that directs the processor to determine the private key and the digital certificate in response to the user authentication data further comprises code that directs the processor to determine a private key not associated with the user when the user authentication data is incorrect.

As discussed above, Arthan merely discloses that it is good to change a public/private key pair if it has been compromised. As noted, Arthan makes no mention of a key wallet and incorrect entry of a password for the key wallet. Arthan discloses a very different problem from what the embodiment described in the present patent specification describes.

In the discussion above, embodiments of the present invention do not refer to key compromise, simply that if a user enters the wrong password to a key wallet, the user will get an inoperative key. There is nothing about the authorized user's key being compromised. Accordingly, the claim language refers to this aspect by reciting that a private key not associated with the user is determined if the user authentication data is incorrect.

In light of the above, these references fail to disclose all the elements of claim 5.

C. Claims 8 and 15

Independent claims 8 and 15 are asserted to be allowable for substantially the same reasons discussed above in claim 1, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

D. Claims 10 and 17

Dependent claims 10 and 17, are asserted to be allowable for substantially the same reasons discussed above for claim 5, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

E. Remaining Claims

Claims 2-7, which depend from claim 1 are also believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

Claims 9-10, 12-14 and 21, which depend from claim 8 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

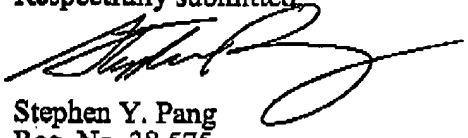
Claims 16-20 which depend from claim 15 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



Stephen Y. Pang
Reg. No. 38,575

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: (650) 326-2400
Fax: (650) 326-2422
SYP:deh
60403582 v1